


Idaho Department of Correction 	Standard Operating Procedure	Title: Computer and Internet Use by Incarcerated Individuals		Page: 1 of 8
		Control Number: 607.26.01.016	Version: 1.0	Adopted: 00/00/2020

Chad Page, chief of the Division of Prisons, approved this document on 04/30/2020.

Open to the public: ☒ Yes

SCOPE

This standard operating procedure (SOP) applies to any Idaho Department of Correction (IDOC) staff member, to include contract staff, involved in the supervision of incarcerated individuals who will be using Stand Alone Computers and internet access.

Revision Summary
Revision date (<u>04/30/2020</u>) version <u>1.0</u> : This is a new SOP detailing the conditions and restrictions required to allow limited computer and internet use by incarcerated individuals for educational purposes on Stand Alone Computers and details the required supervision regarding such use.

TABLE OF CONTENTS

Board of Correction IDAPA Rule Number	1
Policy Control Number 607.....	2
Purpose.....	2
Responsibility	2
Standard Procedures	4
1. General Statement.....	4
2. Eligibility and Approval	5
3. Prohibited Computer/Internet Use	5
4. Mandatory Conditions	6
5. Implementation of Computer Use and/or Internet Access for Incarcerated Individuals ..	6
6. Supervision and Monitoring of Computer Use and/or Internet Access	7
7. Termination of Computer Use and/or Internet Access	7
Definitions	8
References.....	8

BOARD OF CORRECTION IDAPA RULE NUMBER

None

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 2 of 8
---	------------------------	---	-------------------------------

POLICY CONTROL NUMBER 607

Correctional Education and Programs

PURPOSE

The purpose of this standard operating procedure (SOP) is to establish guidelines and requirements for the use of a logically and physically separated network computers and internet access by incarcerated individuals using the Offender Network System (ONS) and Stand Alone Computers.

RESPONSIBILITY

Idaho ITS Services (ITS)

The ITS is responsible for the following regarding the ONS:

- Installing and configuring internet connection(s).
- Implementing security controls.
- Updating internet connections and security controls, as necessary.
- Installing and maintaining computer hardware and software.
- Securing and maintaining appropriate licenses
- Updating hardware, software, as necessary
- Setting up network folders and authorizing access to internet sites approved by IDOC for access by incarcerated individuals
- Blocking access to non-approved internet sites

Idaho Department of Correction (IDOC)

The IDOC is responsible for:

- Ensuring that incarcerated individuals cannot use computers or the internet to access any internal information or any departmental sites or programs.
- Maintaining a list of authorized internet sites and notifying applicable staff of any changes to the list.
- Ensuring that user accounts, user IDs, and passwords are set-up for incarcerated individuals.
- Managing incarcerated individuals' user accounts to include expiration dates, size limitations, etc.
- Ensuring appropriate staff monitor computer use and internet access by incarcerated individuals to improve service levels and prevent unauthorized computer use and/or internet access.
- Ensuring that any security breaches related to incarcerated individuals' computer use and/or internet access are reported and, if necessary, investigated.

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 3 of 8
---	------------------------	---	-------------------------------

- Ensuring that reports of investigations of security breaches are forwarded to appropriate staff.
- Overseeing audits of incarcerated individuals' computer use and internet access.
- Providing any necessary technical assistance to staff who are responsible for supervising computer use and/or internet access by incarcerated individuals.

Division of Prisons Chief

The Division of Prisons chief is responsible for:

- Determining which facilities will allow usage of designated department computers by eligible incarcerated individuals for education and/or reentry planning purposes.
- Determining which facilities will permit limited, monitored internet access on Department computers by eligible incarcerated individuals for education and/or reentry planning purposes.

Division of Prisons Deputy Chief

The deputy chief of the Division of Prisons is responsible for:

- Approving appointments of director of education.
- Ensuring that facilities meet the standards set forth in this SOP.

Director of Education

The director of education is responsible for:

- Reviewing appointments of all education program managers.
- Providing structure to meet the standards set forth in this SOP.
- Authorizing internet sites accessible to incarcerated individuals and educational course approval.

Facility Heads

The facility heads are responsible for:

- Carrying out the requirements of this standard operating procedure.
- Providing enough security staff to create a safe environment.

Education Program Managers

The education program managers are responsible for:

- Supervising instructors and oversight of education program delivery in their respective facilities and monitoring to ensure proper use of computers and internet access.
- Approving incarcerated individuals for computer use and/or limited internet access.

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 4 of 8
---	------------------------	---	-------------------------------

STANDARD PROCEDURES

1. General Statement

Incarcerated Individuals' Computers Use and/or Internet Access Within the Institution:

Education staff must ensure incarcerated individuals accessing computers are aware of all restrictions and limitations that apply regarding use and access to the computer, internet, program or system.

Institutional education staff or other authorized staff are responsible for monitoring and approving incarcerated individuals' computer use and/or internet access by doing the following:

- Incarcerated individuals are only authorized to use, access or view Stand-Alone Computers utilizing hardware and software approved and provided by authorized IDOC staff.
- All computer hardware and software components utilized (including any type of removable data storage device), must remain at the incarcerated individuals' assigned workstation or computer area and must be accounted for by education staff or other authorized staff at the end of each session.
- Incarcerated individuals may only access workstations, systems and programs designated for their use by education staff or other authorized staff.
- Incarcerated individuals' use and access to the education department computers, systems or programs may be withdrawn at any time.
- All IDOC staff members authorized to use state-owned computers capable of accessing the state intranet/external internet located in areas where incarcerated individuals could potentially gain access to the computer are responsible for the security of information on the computer and confidentiality of their logon identification (user ID and password(s)). Staff must never divulge confidential information to incarcerated individuals. Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.
 - Staff must change their computer log on password if they suspect the confidentiality of their password has been compromised.
 - Staff assigned to state owned computers in areas accessible to incarcerated individuals must ensure the computer LOCK device is enabled (by pressing <Ctrl> <Alt><Delete> on the keyboard) when the computer is not in use by the staff member, or the staff member's workstation is unattended.
- Incarcerated individuals are prohibited from using, accessing, viewing or interacting (directly or indirectly) with computers, systems, programs (including internet and/or electronic media) for personal business or pleasure, e.g. legal work, writing personal letters, playing computer games, listening to music, accessing, viewing or interacting with email, instant messaging, social media or viewing unapproved internet sites.

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 5 of 8
---	------------------------	---	-------------------------------

- Incarcerated individuals are prohibited from repairing or modifying any state owned or leased computer equipment, hardware, software, system(s) or program(s), except as part of an authorized training program or when an exemption has been granted by the facility head or their designee.
- Incarcerated individuals permitted to use computers must not engage in inappropriate, offensive or illegal activities or violate institutional rules and should not expect privacy or confidentiality when using a computer.

2. Eligibility and Approval

An incarcerated individuals enrolled in a department approved educational course may be approved for:

- Computer use if computer use is necessary for accomplishing the required work.
- Limited internet access if required to accomplish specific tasks or required work, including access to applicable online college resource(s), e.g., online writing labs, etc.

Incarcerated individuals may also be approved for limited computer use and/or internet access if they are engaged in a department-approved reentry plan in which computer use and/or internet access is necessary for facilitating reentry.

3. Prohibited Computer/Internet Use

An incarcerated individual approved for computer use and/or limited internet access is prohibited from using a computer or the internet:

- To violate copyright laws.
- To harass or threaten anyone.
- For any other illegal activity.
- To commit a disciplinary violation.
- To access pornography.
- To access any materials that would not be allowed to be received via the mail as set out in SOP [402.02.01.001](#), *Mail Handling in Correctional Facilities*.
- To upload any program or introduce any virus into any computer, system, or program.
- To impersonate any other person, falsely represent them self, or make any other false statement in connection with computer use or internet access.
- To intentionally or negligently destroy or damage or cause a malfunction of any computer, peripheral equipment and not consume food and/or beverages when using or around a computer or peripheral equipment.
- To contact anyone with whom they have a no contact order or who is a victim of a crime committed by them.

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 6 of 8
---	------------------------	---	-------------------------------

- To contact anyone on behalf of another incarcerated individual for any reason.
- On behalf of another incarcerated individual or allowing another incarcerated individuals to access to that individual's user account, user ID, password, or USB drive/flash drive, if applicable.

4. Mandatory Conditions

Computer use and/or internet access by incarcerated individuals is not confidential and may be viewed or otherwise monitored by appropriate staff at any time.

Any incarcerated individual who violates any of these conditions is subject to termination of approval for computer use and/or internet access, disciplinary or other administrative action, and/or criminal prosecution.

To comply with these mandatory conditions, an incarcerated individual:

- May only use workstations and computers designated for use by incarcerated individuals.
- Must not access any internet site that is not authorized by the Department.
- May only use a computer and/or access the internet for authorized purposes as specified in their case plan.
- Is never authorized by a case plan to use a computer and/or access the internet for conducting business activities, doing legal work, writing personal letters, playing computer games, listening to music, instant messaging, or accessing social media or chat rooms.
- Cannot use or possess a USB drive/flash drive unless approved.
- Cannot download or print documents unless authorized by the facility staff supervising the educational program or reentry planning, as applicable.
- Is not allowed to repair or modify any computer or peripheral equipment, USB drive/flash drive, software, system, or program, except as part of a Department approved training program or when specific approval has been granted by the educational program manager or supervisor.
- Is required to exit all applications and log off the computer when finished using the computer.
- Is responsible for compensating the Department for any losses, costs, or damages to a department computer, peripheral equipment, USB drive/flash drive, software, system, or program due to their intentional act or negligence.
- Is required to immediately report to staff supervising the program any inadvertent access to any site or material that is not authorized.

5. Implementation of Computer Use and/or Internet Access for Incarcerated Individuals

Upon receiving approval for an incarcerated individual to use a computer and have limited internet access, the designated staff member will:

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 7 of 8
---	------------------------	---	-------------------------------

- Set up the incarcerated individual's user account.
- Assign the incarcerated individual a user ID and password(s), if applicable. The staff member will maintain a list of assigned user IDs and passwords.
- Issue the incarcerated individual a USB drive/flash drive, if applicable. The staff member will maintain a list of assigned USB drives/flash drives issued.

6. Supervision and Monitoring of Computer Use and/or Internet Access

Designated education staff will manage incarcerated individuals' use of computers and limited internet access by setting usage priorities as described in SOP [607.26.01.012](#), *Educational Practices, Procedures, and Placements*.

- Designated education staff will remind users of the mandatory conditions and any additional conditions for computer use and, if applicable, internet access and/or use of a USB drive/flash drive.
- For incarcerated individuals who have not been issued a USB drive/flash drive but are allowed the use of one in the classroom for approved education purposes, only designated education staff may handle the USB drive/flash drive. The staff will maintain a signed log for each session, which will include the individual's name and IDOC number, the purpose for the use, and the date and times during which the drive is used.
- Designated education staff will monitor computer use and/or internet access by the incarcerated individual to ensure appropriate use. Security staff may also monitor computer use and/or internet access to ensure appropriate use. As part of the monitoring, staff may inspect a computer, a USB drive/flash drive, electronic files, downloaded or printed material, internet sites accessed, etc. at any time for any reason.
- If any staff becomes aware of or suspects that an incarcerated individual has violated any condition of computer use and/or internet access, the staff must act immediately to stop any ongoing violation. The staff will take appropriate actions in response to any violation, including, but not limited to, suspending their computer use or internet access, initiating disciplinary action, and reporting the violation to the appropriate staff. If criminal activity is suspected, the staff will secure and preserve the computer, peripheral equipment, and the USB drive/flash drive, if applicable, in its current state and immediately notify the security staff.
- Education staff must ensure that computers are kept secured from any access by incarcerated individuals when the computers are not authorized for use.

7. Termination of Computer Use and/or Internet Access

Access by incarcerated individuals to computers and limited internet use is only associated with IDOC's educational programs and can be terminated at any time. If computer use and/or internet access has been terminated, education staff, or designated staff, must cancel the user account and confiscate the USB drive/flash drive issued, if applicable.

Incarcerated individuals' computer use and internet access will also be terminated when:

Control Number: 607.26.01.016	Version: 1.0	Title: Computer and Internet Use by Incarcerated Individuals	Page Number: 8 of 8
---	------------------------	---	-------------------------------

- They are released from institutional confinement or transferred to a facility or placed in a housing unit that either does not provide or will not allow computer use or internet access.
- They are no longer enrolled in a course and will not be enrolled in a course requiring computer or internet access, in the immediate or upcoming enrollment, as applicable.
- They are no longer involved in reentry planning classes.
- There is any violation of conditions described in this SOP or at the discretion of IDOC staff, following guidelines in SOP [318.02.01.001](#), *Disciplinary Procedures for Inmates*.

DEFINITIONS

Intranet: The IDOC network provides information on department policies and procedures, development services, standards and tools, electronic government and other internal resources within the department. The network is an internal online information technology infrastructure throughout state government and is available to employees of state government.

Offender Network System (ONS): Logically and physically separated network allowing incarcerated individuals to have limited, controlled, access to internet connected resources. The ONS applies to any networked connected device that incarcerated individuals have access to. Devices include, but are not limited to, workstations, tablets, kiosks, or cell phone technology. Any device accessed or used by incarcerated individuals must only connect to an ONS.

Social Media: Includes but is not limited to print, broadcast, digital and online services such as Facebook, LinkedIn, Twitter, among others.

Stand-Alone Computer: A computer not tied into a State Local Area Network (LAN) system or the State's Wide Area Network (WAN), a computer that connect to the Intranet.

REFERENCES

Standard Operating Procedure [318.02.01.001](#), *Disciplinary Procedures for Inmates*

Standard Operating Procedure [402.02.01.001](#), *Mail Handling in Correctional Facilities*

Standard Operating Procedure [607.26.01.012](#), *Educational Practices, Procedures, and Placements*

– End of Document –